2018
ANNUAL REPORT
COOPERATION & TRANSPARENCY

edpb
European Data Protection Board

European Data Protection Board
2018 Annual Report

Cooperation & Transparency

An Executive Summary of this report, which gives an overview of key developments in EDPB activities in 2018, is also available.

Further details about EDPB can be found on our website at edpb.europa.eu.

TABLE OF CONTENTS

Foreword

2018 was a landmark year for data protection. On 25 May 2018, the long anticipated General Data Protection Regulation (GDPR) entered into application. In addition to updating the European Union's data protection rules for the digital age, this Regulation established the European Data Protection Board (EDPB) to ensure consistent application of the new rules across the EEA.

The EDPB is therefore a young EU body. Yet even in the first seven months of its existence, we have reached several milestones which we are now able to reflect upon.

Our role is to ensure the harmonised enforcement of the GDPR across the EEA. To this end, we endorsed the 16 GDPR related Guidelines of the Article 29 Working Party, we adopted 4 more Guidelines, 26 Opinions on Data Protection Impact Assessments carried out by the national Supervisory Authorities and held five plenary meetings addressing a range of topics, from the EU-Japan draft adequacy decision to electronic evidence and ePrivacy.

The feedback we have received from stakeholders on the first year of work has been encouraging. Many people and companies are now calling for increased global alignment on the processing of personal data. We believe that by coordinating a consistent approach to data protection, the EU is demonstrating that respect for individuals' rights to privacy and data protection can go hand-in-hand with a flourishing economy, not least because it provides businesses with a clear framework and creates competitive advantages, such as improved customer loyalty and more efficient operations.

Next year is set to be even busier. At the beginning of 2019, we adopted our working programmes for 2019-2020. The EDPB work programme aims to address the priority needs of all stakeholders, including EU legislators. Having already issued guidance on the interpretation of new provisions introduced by the GDPR, the EDPB will now turn its attention to specific items and technologies.

In my view, with national Supervisory Authorities working together on an equal footing and the support of a dynamic Secretariat, the EDPB is well equipped for its mission of upholding a high level of data protection across the EEA. Looking ahead, I am confident that we will continue to lead by example in striving for transparency and cooperation in the EEA, and beyond.

Andrea Jelinek
Chair of the European Data Protection Board

2

Mission statement, tasks and principles

The European Data Protection Board (EDPB) aims to ensure the consistent application of the General Data Protection Regulation (GDPR) and of the European Law Enforcement Directive across the Economic European Area.

The EDPB can adopt general guidance to further clarify European data protection laws, giving stakeholders – including individuals – a consistent interpretation of their rights and obligations, and providing Supervisory Authorities with a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Decisions (more precisely, 'Consistency Opinions' or 'Consistency Decisions') to guarantee a consistent application of the GDPR across the EEA by the national Supervisory Authorities.

The EDPB acts in accordance with its rules of procedure and guiding principles.

2.1. TASKS AND DUTIES

- The EDPB provides general guidance (including guidelines, recommendations and best practices) to clarify the law.
- The EDPB issues **Consistency** Opinions or Decisions to guarantee the consistent application of the GDPR.
- The EDPB promotes **cooperation** and the effective exchange of information and best practices between national Supervisory Authorities.
- The EDPB **advises** the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union.

2.2. GUIDING PRINCIPLES

- **Independence and impartiality.** The EDPB is an independent body, which performs its tasks and exercises its powers impartially.
- **Good governance,** integrity and good administrative behaviour. The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with good decision-making processes and sound financial management.
- **Collegiality and inclusiveness.** The EDPB is organised and acts collectively as a collegiate body, as established by the provisions of the GDPR and the Police and Criminal Justice Data Protection Directive.
- **Cooperation.** The EDPB promotes cooperation between Supervisory Authorities and endeavours to operate, where possible, by consensus, holding the GDPR and the Data Protection Directive as an overarching reference.
- **Transparency.** The EDPB carries out its work as openly as possible, so as to be more effective and more accountable to the public. The EDPB strives to explain its activities using clear language that is accessible to all.
- **Efficiency and modernisation.** The EDPB makes every effort to ensure that its work is as efficient and as flexible as possible, in order to achieve the highest level of cooperation between its members. The EDPB does this by using new technologies to keep working methods up to date, minimise formalities, and provide efficient administrative support.
- **Proactivity.** The EDPB undertakes its own initiatives, in order to anticipate and support innovative solutions that will help to overcome digital challenges to data protection. The EDPB encourages the effective participation of stakeholders (whether members, observers, staff or invited experts), so that their needs and aspirations can be fully taken into account.

3

About the European Data Protection Board

The European Data Protection Board is an independent European body, which contributes to the consistent application of data protection rules throughout the European Economic Area and promotes cooperation between the EEA's Data Protection Authorities.

The EDPB is composed of representatives of the national Data Protection Authorities and the European Data Protection Supervisor (EDPS). The Supervisory Authorities of the EEA EFTA States (Iceland, Liechtenstein and Norway) are also members with regard to GDPR-related matters, although they do not hold the right to vote nor can they be elected as chair or deputy chair.

The EDPB was established by the General Data Protection Regulation (GDPR). The European Commission and – with regard to GDPR-related matters – the European Free Trade Association (EFTA) Surveillance Authority have the right to participate in the activities and meetings of the Board, but without voting rights.

The EDPB has a Secretariat, which is provided by the EDPS. A Memorandum of Understanding determines the terms of cooperation between the EDPB and the EDPS.

4

2018 – an overview

4.1. SETTING UP THE EDPB

4.1.1 The Rules of Procedure

The rules of procedure were adopted during the first plenary meeting of the European Data Protection Board, which took place on 25 May 2018. These outline the most important operational rules of the Board. They describe:

- The EDPB's guiding principles
- The organisation of the EDPB
- The cooperation between its members
- The election of its chair and deputy chairs
- The EDPB's working methods

On 23 November 2018, the EDPB approved several changes to its rules of procedure. Among other things, the changes gave full effect to the European Economic Area (EEA) Joint Committee decision, integrating the General Data Protection Regulation (GDPR) into the EEA agreement. The EEA EFTA Supervisory Authorities participate fully within the EDPB, without the right to vote or to be elected as chair or deputy chair.

4.1.2. Organisation of Expert Subgroups

To assist in performing its tasks, several expert subgroups have been set up within the EDPB.

The establishment, suspension or termination of any expert subgroup may be decided upon at any time, following a proposal from the Chair or from at least three members of the Board. The list of expert subgroups is reviewed by the Board in the first plenary meeting of each year.

The list of the expert subgroups and their respective mandates are available under section 11.2.

4.2. SETTING UP THE SECRETARIAT

4.2.1. Memorandum of Understanding

The Memorandum of Understanding (MoU) determines the terms of cooperation between the European Data Protection Board and the European Data Protection Supervisor (EDPS). While the EDPS is a member of the EDPB, it also provides the Secretariat to the EDPB. The GDPR states that the Secretariat is required to perform all its tasks exclusively under the instructions of the Chair. These tasks involve providing analytical, administrative and logistical support to the EDPB.

The MoU establishes a clear separation between the functions assigned specifically to the EDPB Secretariat and the administrative support functions provided to the Secretariat by the EDPS, such as those related to human resources, working equipment, finance and budget. The EDPB Secretariat is in charge of the organisation of EDPB meetings and analytical support by drafting EDPB documents, as well as content-related duties, such as record management, the handling of access requests, local information security, public and press communications and the duties of the data protection officer.

In the interest of sound administration and consistent cooperation, the terms of the MoU were agreed upon by both the EDPB and the EDPS prior to the entry into force of the GDPR, during the first EDPB plenary meeting on 25 May 2018.

4.2.2. Preparation for 25 May 2018

To set up the EDPB Secretariat ahead of 25 May 2018, a dedicated EDPB Matters sector was created within the EDPS. Throughout 2017 and early 2018, this sector was responsible for carrying out the preparatory measures needed to create the EDPB. These included selecting and customising IT communication tools, preparing the EDPB's external communications, concluding agreements with other EU institutions for the externalisation of certain activities and developing legal agreements in cooperation with the national Supervisory Authorities (including the Memorandum of Understanding and the Rules of Procedure).

4.3. SETTING UP COOPERATION AND CONSISTENCY

4.3.1. IT Communications Tool (IMI)

Under the GDPR, the Supervisory Authorities (SAs) of EU Member States cooperate closely to ensure consistent protection of individuals' data protection rights across the European Union. One of their tasks is to assist one another and coordinate decision-making in cross-border data protection cases. Via the so-called consistency mechanism, the EDPB issues Consistency Opinions or Decisions. The EDPB binding Consistency Decisions aim to arbitrate in cases where national Data Protection Authorities take different positions in cross-border cases.

Via the so-called consistency mechanism, the EDPB issues Consistency Opinions or Decisions.

The Internal Market Information System (IMI) was chosen as the IT platform to support cooperation and consistency procedures under the GDPR. IMI helps public authorities cooperate and exchange information. The GDPR is the thirteenth legal area supported by the system.

IMI was developed by the European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). It has been adapted, in close cooperation with the EDPB Secretariat and in consultation with the national Supervisory Authorities, to suit the needs of the GDPR. Fourteen IMI modules, 19 forms and more than 10,000 data fields have been created to address the needs of Data Protection Authorities and the GDPR procedures.

On 25 May 2018, the first case was initiated in IMI and shortly afterwards Supervisory Authorities started to cooperate via the system. By the end of 2018, more than 255 cross-border cases were being examined.

5

European Data Protection Board activities in 2018

The EDPB aims to ensure the consistent application of the General Data Protection Regulation (GDPR) and of the European Law Enforcement Directive across the European Union.

The EDPB can adopt general guidance to clarify European data protection laws. This provides stakeholders with a consistent interpretation of their rights and obligations and ensures that Supervisory Authorities have a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by the national Supervisory Authorities.

5.1. GENERAL GUIDANCE

During its first plenary meeting on 25 May 2018, the EDPB **endorsed 16 Guidelines** previously established by the Article 29 Working Party (WP29) (see Annex for full list).

During the remainder of 2018, the EDPB adopted four more Guidelines that aim to clarify a range of provisions under the GDPR. These Guidelines address certification and the identification of certification criteria, derogations relating to international transfers, the territorial scope of the GDPR and the accreditation of certification bodies.

5.1.1. Guidelines on Certification and identifying Certification Criteria

During its first plenary meeting on 25 May 2018, the EDPB adopted a first version of the Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

The EDPB's guidance provides stakeholders with a consistent interpretation of their rights and obligations.

Achieving certification from an approved certification body is an element that may be used by organisations to demonstrate their compliance with EU data protection legislation.

As early as 2010, the Article 29 Working Party established that certification could play an important role in the accountability framework for data protection. The GDPR reinforced this principle, stating that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation.

However, certification remains a voluntary process. The EDPB has therefore encouraged Member States and Supervisory Authorities (SAs) to establish certification mechanisms and provided guidance to clarify the role of SAs in this process.

Following the adoption of the first version of the document, a public consultation was launched and remained open for six weeks. A final version of the Guidelines was adopted in December 2018, taking into account the results of the consultation.

5.1.2. Guidelines on Derogations Applicable to international Transfers

During its first plenary meeting, the EDPB adopted the Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679 applicable to international transfers that clarify how to interpret the derogations outlined under Article 49. The guidelines clarify the need to interpret those derogations in a restrictive manner, as they are exceptions to the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.

The Guidelines build on the work of the Article 29 Working Party, which conducted a public consultation on an initial version of the text. The EDPB took into consideration the input received and integrated the appropriate changes into the final version.

5.1.3. Guidelines on Territorial scope

Article 3 of the GDPR determines the territorial scope of the Regulation and seeks, in the context of worldwide data flows, to establish a level playing field for companies operating in the EU. The territorial scope of the GDPR is based on two main criteria: the "establishment" criterion, outlined in Article 3(1), and the "targeting" criterion, outlined in Article 3(2).

The relevant provisions of the GDPR apply depending on which of these criteria are met. The "establishment" criterion refers to cases in which a controller or processor is established within the EU, regardless of whether the actual processing of personal data takes place in the EU or not. The "targeting" criterion applies to cases where a controller or processor is not established within the Union, but in which the processing of personal data involves offering goods or services to individuals in the EU or monitoring their behaviour.

During its fourth plenary meeting on 16 November 2018, the EDPB adopted a first version of the Guidelines 03/2018 on the territorial scope of the GDPR, with the aim of providing a common interpretation for the application of these criteria. The Guidelines specify the various scenarios that may arise and how to address them. These include cases where the data controller or processor is established outside of the EU and cases in which the designation of a representative in the EU is required.

The Guidelines were subject to a public consultation.

5.1.4. Guidelines on Accreditation

During its fifth plenary meeting on 4 December 2018, the EDPB adopted a revised version of the Guidelines 04/2018 on the accreditation of certification bodies. The first version of the guidelines was adopted by the Article 29 Working Party and the revised version aimed to incorporate the feedback received during the public consultation. This issue of accreditation is addressed by Article 43 of the GDPR, which requires Member States to ensure that certification bodies responsible for issuing GDPR certifications are accredited by either or both the competent Supervisory Authority or the relevant national accreditation body. In cases where accreditation is carried out by the national accreditation body, the Article sets out the additional requirements that must also apply. The EDPB Guidelines aim to clarify the accreditation process.

A public consultation was held on the first version of the text by the Article 29 Working Party. The EDPB also adopted a new Annex providing guidance on the additional accreditation requirements to be established by the national Supervisory Authorities. This annex was subject to a new public consultation.

5.2. CONSISTENCY FINDINGS

5.2.1. Consistency Opinions

EEA national SAs must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR having cross-border implications. This applies when a national SA:

- intends to adopt a list of the processing operations subject to the requirement for a data protection impact assessment (DPIA);
- intends to adopt a draft code of conduct relating to processing activities;
- aims to approve the criteria for accreditation of a certification body;
- aims to adopt standard data protection clauses or contractual clauses;
- aims to approve binding corporate rules.

The competent Supervisory Authority has to take utmost account of the opinion.

In addition, any Supervisory Authority, the Chair of the Board or the Commission may request that any matter of general application or which has consequences for more than one Member State be examined by the Board with a view to obtaining an Opinion. This can also apply in cases where a competent Supervisory Authority does not comply with obligations for mutual assistance or for joint operations.

The aim of these Opinions is to guarantee the consistent application of the GDPR by the national Supervisory Authorities.

Between 25 May and 31 December 2018, 26 Consistency Opinions on the national lists of processing operations subject to a DPIA were adopted by the EDPB. The purpose of the exercise was to ensure consistency across all national lists.

5.2.2. Binding Decisions

The EDPB can also act as a dispute resolution body. It adopts binding decisions to ensure the consistent application of the GDPR by the national Supervisory Authorities in the following cases:

- a dispute takes place within the One-Stop-Shop mechanism (a Concerned SA raises a relevant and reasoned objection which is not followed by the Lead SA);
- a disagreement occurs relating to which authority should take on the role of Lead SA;
- an SA does not request, or does not follow, a Consistency Opinion issued by the EDPB.

For more information on the operations of Lead SAs versus Concerned SAs, please see Chapter 6 of this report.

Between 25 May and 31 December 2018, no dispute resolutions were initiated. This suggests that, to date, SAs have been able to reach consensus on all current cross-border cases.

5.3. LEGISLATIVE CONSULTATION

The EDPB advises the European Commission on any issue related to the protection of personal data, on the format and procedures for information exchange between companies and SAs under Binding Corporate Rules (BCRs) and on certification requirements. The EDPB also advises the European Commission on the assessment of the adequacy of the level of data protection in third countries or international organisations.

In 2018, the EDPB issued two such Opinions: one on electronic evidence (e-Evidence) and one on the EU-Japan draft adequacy decision. The European Commission requested both of these Opinions.

As of 11 December 2018 - when the new data protection rules for the EU institutions came into force - the EDPB is also subject to Article 42 of Regulation 2018/1725 on legislative consultation. This allows for the EDPS and the EDPB to coordinate their work, with the intention of issuing a joint Opinion.

In 2018, the EDPB also adopted, on its own initiative, a statement on the draft ePrivacy Regulation.

5.3.1. e-Evidence

During its Third Plenary Session, which took place on 25 and 26 September 2018, the EDPB adopted the Opinion 23/2018 on the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, proposed by the European Commission in April 2018.

The EDPB stressed that the proposed new rules providing for the collection of electronic evidence should sufficiently safeguard individuals' data protection rights whilst aligning more closely with EU data protection law.

5.3.2. EU-Japan draft adequacy decision

During the Fifth Plenary Session of the EDPB, which took place on 4-5 December 2018, the EDPB Members adopted the Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, which the EDPB received in September 2018.

The EDPB's key objective was to assess whether the European Commission had ensured that the Japanese framework provided for an adequate level of data protection for individuals, essentially equivalent to the standard set out in the GDPR. The EDPB made its assessment based on the documentation provided by the Commission.

The GDPR requires that, in order to be considered adequate, any non-EU country's legislation must be aligned to the principles and concepts enshrined in the GDPR, as well as to general aspects of EU law, including the rule of law.

There were key areas of alignment between the GDPR framework and the Japanese framework on certain core

provisions. In addition, the EDPB welcomed the efforts made by the European Commission and the Japanese Personal Information Protection Commission (PPC) to increase this convergence.

However, the EDPB noted that a number of concerns remained, particularly relating to the notion of consent, which includes the right to withdraw consent, to transparency obligations and to access to the redress system. The EDPB also requested further clarification on the role of the data processor and on the extent of the restrictions to the rights of individuals set out in Japanese legislation, as well as assurance that personal data transferred from the EU to Japan would be closely monitored during the whole "life cycle" of the transfer.

Some of those elements were taken into account in the revised adequacy decision adopted by the European Commission on 23 January 2019.

5.3.3. Statement on ePrivacy

During its first plenary meeting of 25 May 2018, the EDPB adopted a statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.

This statement includes a call for a swift adoption of the new ePrivacy Regulation and some suggestions on some specific issues relating to proposed amendments by the co-legislators.

5.4. OTHER DOCUMENTS

5.4.1. Letter to ICANN

During the Second Plenary Session of the EDPB, on 4 and 5 July 2018, the EDPB adopted a letter addressed to Mr Göran Marby, President and CEO of the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN). The letter provided guidance to help ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS. The WHOIS system provides a register for domain names and IP addresses.

The letter addressed the issues of purpose specification, collection of "full WHOIS data", registration of legal persons, logging of access to non-public WHOIS data, data retention and codes of conduct and accreditation.

The EDPB expects ICANN to develop and implement a WHOIS model that will enable the legitimate use of personal data concerning those registered in the WHOIS system, specifically by relevant stakeholders such as law enforcement, without leading to an unlimited publication of such data.

5.4.2. Letter on the PSD2 Directive

The EDPB adopted a second letter in July 2018. Addressed to Sophie in't Veld, Member of the European Parliament, it aimed to respond to her request for further clarification on a number of issues relating to the revised Payments Services Directive (PSD2 Directive) and the protection of personal data. The PSD2 Directive concerns payment services in the EU's internal market. In this letter, the EDPB aimed to clarify:

- the concept of "silent party data" and the processing of this data by Third Party Providers;
- procedures for giving and withdrawing consent;
- Regulatory Technical Standards;
- cooperation between banks and the European Commission, the EDPS and the WP29;
- any other data protection gaps remaining.

The EDPB also expressed its wish for a dialogue between competent EU bodies (particularly data protection and financial Supervisory Authorities) in order to set up a coordinated approach aimed at ensuring strengthened and consistent protection for EU citizens.

5.4.3. Statement on Economic Concentration

In August 2018, the EDPB adopted a statement on the impact of economic concentration on data protection via written procedure. The statement followed the European Commission's announcement that it intended to analyse the effects of further concentration of 'commercially sensitive data about customers' personal data in the context of its investigation into the proposed acquisition of Shazam by Apple. The EDPB considered it essential to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed, particularly in technology sectors of the economy. The Board went on to note that increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services. The data protection and privacy interests of individuals are relevant to any assessment of potential abuse of dominance as well as mergers of companies, which may accumulate or which have accumulated significant informational power. The statement concluded that independent Data Protection Authorities can help with the assessment of such an impact on the consumer or society more generally in terms of privacy, freedom of expression and choice.

5.5. PLENARY MEETINGS AND EXPERT SUBGROUPS

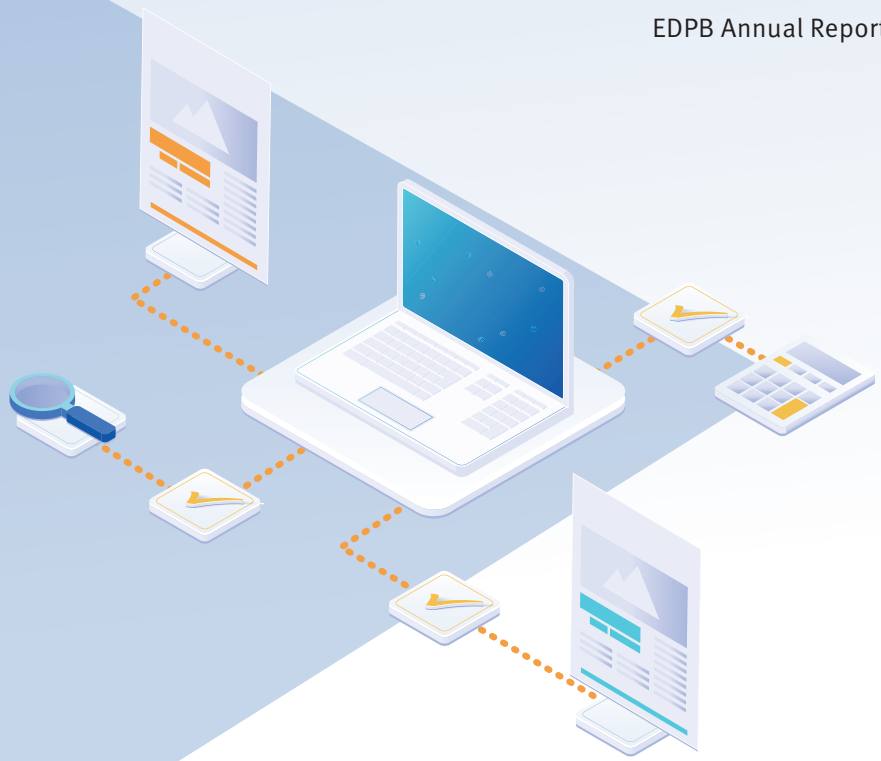
Between 25 May and 31 December 2018, the EDPB held five plenary sessions. During these sessions the EDPB Members adopted guidance and requests for mandates for the relevant expert subgroups and practical matters related to the functioning of the Secretariat.

In addition, there were 36 expert subgroup meetings. The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks.

The list of the expert subgroups and their respective mandates are available below in section 11.2.

The EDPB expressed its wish for a dialogue between competent EU bodies aimed at ensuring strengthened protection for EU citizens.

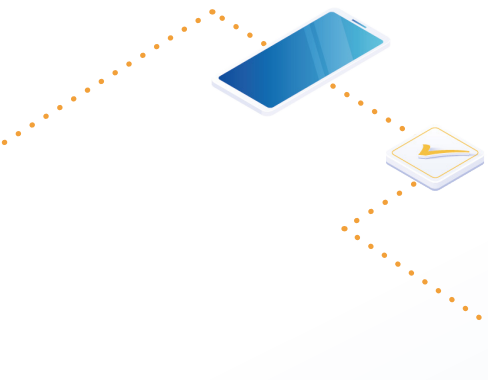
6



Supervisory Authority activities in 2018

Under the GDPR, the Supervisory Authorities have a duty to cooperate in order to ensure consistent application of the Regulation. In cases with a cross-border component, the Supervisory Authorities of the European Economic Area (the 28 EU Member States plus Iceland, Norway and Liechtenstein) have a range of tools at their disposal to facilitate harmonisation. These are:

- mutual assistance;
- joint operation;
- the One-Stop-Shop cooperation mechanism.



6.1. CROSS-BORDER COOPERATION

6.1.1. Preliminary Procedure to Identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop procedure for a cross-border case, it is necessary to identify the authority that will lead the investigation (Lead SA) and the other Concerned Supervisory Authorities (Concerned SA or SAs). The Lead SA will lead the investigation and draft the decision, while the Concerned SAs will have the opportunity to raise objections.

The Lead SA is the authority within the EEA where the controller or processor under investigation has its main establishment. For example, the place of central administration is one of the criteria used to identify the main establishment of a controller or processor.

The Lead SA is the authority within the EEA where the controller or processor under investigation has its main establishment.

Further information on this subject is available in Article 1.2 of the Article 29 Working Party Guidelines on identifying a controller or processor's lead Supervisory Authority.

The EDPB created workflows in the Internal Market Information (IMI) system to enable the SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define their roles at an early stage and to avoid objections relating to competencies later on.

In case of conflicting views regarding which authority should act as Lead SA, the EDPB will act as a dispute resolution body and will issue a binding decision.

In 2018, 574 procedures were initiated to identify the Lead SA and the Concerned SAs in cross-border cases. Of these 574 procedures, 274 have been closed.

In 2018, no dispute on the selection of the Lead SA occurred.

6.1.2. Database Regarding Cases with a Cross-Border Component

A cross-border case emerges where the controller or the processor has an establishment in more than one Member State, or where the data processing activity substantially affects individuals in more than one Member State.

Cases with a cross-border component are registered in a central database from which the aforementioned procedures can be initiated.

Between 25 May and 31 December 2018, 255 cases with a cross-border component were registered in the IMI system. Most of the cases derived from complaints by individuals (176 cases). The rest (79 cases) originated from other sources, such as an investigation, an SA initiative, a legal obligation or a media report.

The three main topics of these cases related to data subjects' rights, consumer rights, and data breaches.

In case of conflicting views regarding which authority should act as Lead SA, the EDPB will act as a dispute resolution body and will issue a binding decision.

6.1.3. One-Stop-Shop Mechanism

The GDPR establishes a specific cooperation procedure (One-Stop-Shop) for cross-border cases.

The One-Stop-Shop mechanism demands cooperation between the Lead SA and the Concerned SA. The Lead SA leads the investigation and plays a key role in the process of reaching consensus between the Concerned SAs, in addition to working to reach a coordinated decision with regard to the data controller or processor.

The Lead SA must first investigate the case while observing national procedural rules, ensuring that the affected individuals are able to exercise their right to be heard, for example. During this investigation phase, the Lead SA can gather information from another Supervisory Authority via mutual assistance or by conducting a joint investigation.

If a dispute arises on the draft decision and no consensus can be found, the consistency mechanism is triggered and the case is referred to the EDPB.

The IMI system also gives the Lead SA the opportunity to launch informal communication with all Concerned SAs, in order to collect information.

Once the Lead SA has completed its investigation, it prepares a draft decision and communicates it to the Concerned SAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, triggers the EDPB's dispute resolution mechanism.

If a dispute arises on the draft decision and no consensus can be found, the consistency mechanism is triggered and the case is referred to the EDPB. The EDPB will then act as a dispute resolution body and issue a binding decision on the case. The Lead SA must adopt its final decision on the basis of the EDPB's decision.

If the Concerned SAs do not object to the initial draft decision, or to the revised one, they are deemed in agreement with the draft decision.

The IMI system offers different procedures to follow when handling One-Stop-Shop cases:

- informal consultation procedures;
- draft decisions or revised decisions submitted by the Lead SA to the Concerned SAs;
- final One-Stop-Shop decisions submitted to the Concerned SAs and to the EDPB.

Between 25 May and 31 December 2018, 43 One-Stop-Shop procedures were initiated by SAs from 14 different EEA countries. At the end of the year, the procedures were at different stages: 20 were at the informal consultation level, 20 were at draft decision level and two were final decisions.

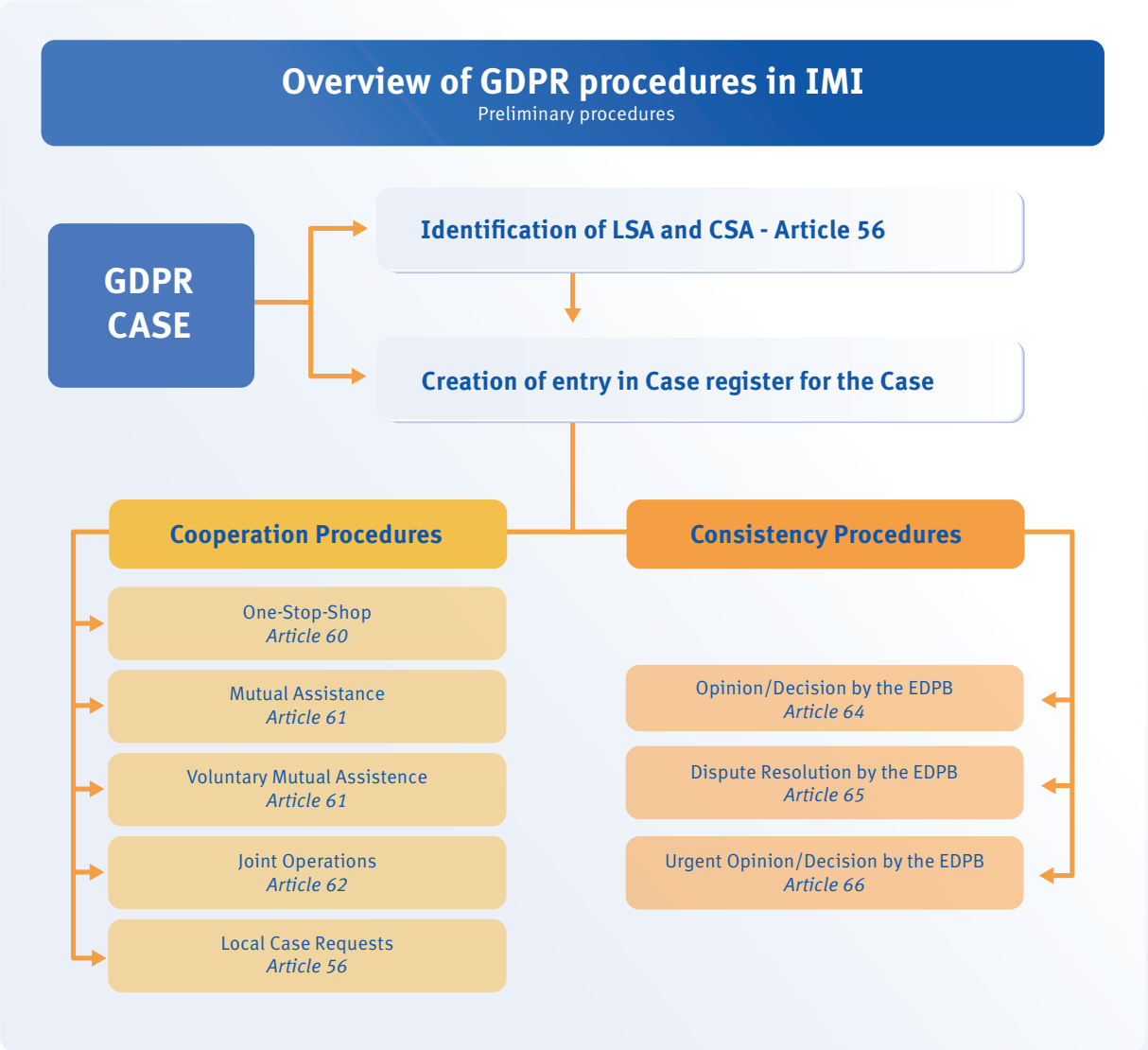
These first One-Stop-Shop final decisions related to the exercise of the rights of individuals (such as the right to erasure), the appropriate legal basis for data processing and data breach notifications.

The limited number of One-Stop-Shop procedures to date can be explained by the fact that the draft decisions produced by Lead SAs result from the investigations they have conducted with respect to the relevant national administrative procedural laws. However, an increase has been observed in the number of One-Stop-Shop procedures being launched.

6.1.4. Mutual assistance

The mutual assistance procedure allows for Supervisory Authorities to ask for information from other SAs, but also to request other measures for effective cooperation, such as prior authorisations or investigations.

Mutual assistance can be used for cross-border cases subject to the One-Stop-Shop procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision, or for national cases with a cross-border component.



The IMI system enables the use of either informal mutual assistance without any legal deadline or the use of formal mutual assistance, whereby the SA from which information has been requested has a legal deadline of one month to reply.

In the period between 25 May and 31 December 2018, 397 mutual assistance requests, both formal and informal, were triggered. 89% of the requests were replied to within 23 days.

6.1.5. Joint operations

The GDPR allows for Supervisory Authorities to carry out joint investigations and joint enforcement measures. Similarly to the mutual assistance procedure, joint operations can be used in the context of cross-border cases subject to the One-Stop-Shop procedure or for national cases with a cross-border component.

6.2. NATIONAL CASES

In 2018, the Supervisory Authorities of the 31 EEA countries reported over a hundred thousand cases at national level. The majority of cases were either related to complaints or were initiated on the basis of data breach notifications from controllers.

Supervisory Authorities have different corrective measures at their disposal. These are:

- issuing warnings to a controller or processor that intended processing operations are likely to infringe the GDPR;
- issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- ordering the controller or processor to comply with the data subject's requests or to bring processing operations into compliance with the GDPR;
- imposing administrative limitations, bans or fines.

6.2.1. Some relevant national cases with exercise of corrective powers[1]

6.2.1.1. Austria

On 12 September 2018, the Austrian Data Protection Authority (DPA) took its first administrative penal decision relating to infringements of the GDPR and the Austrian Data Protection Act.

The Austrian DPA imposed a fine on a Limited Liability Company running a sports betting café. This company was defined, within the meaning of Article 4(7) of the GDPR, as the controller of an image processing system, specifically, video surveillance. The cameras in question had been in use at least since 22 March 2018.

The Austrian DPA found that the controller violated several articles of the GDPR as well as provisions of the Austrian Data Protection Act (DSG), since public areas were involved in the surveillance but the company failed to delete any of the personal image data recorded. The Limited Liability Company was therefore issued with administrative fines amounting to 5,280 EUR.

The controller lodged a complaint with the Federal Administration Court appealing this decision.

6.2.1.2. Germany

On 21 November 2018, the Supervisory Authority of **Baden-Württemberg** imposed the first German fine under the GDPR. Due to a violation of Article 32 of the GDPR on the Security of Processing, a German social network operator was fined 20,000 EUR.

The company had notified the Supervisory Authority of a data breach occurring in July 2018, in accordance with Article 33 of the GDPR. In their notification, they reported that the personal data of 330,000 users, such as e-mail addresses and passwords, had been hacked. The company cooperated fully and provided information on internal structures, which showed that passwords had been stored unencrypted. The company thereby failed to ensure data security according to Article 32(a) of the GDPR.

Due to its exemplary cooperation and readiness to follow all of the SA's recommendations, and taking into account the financial burden of the implementation costs and the initial fine, the company was not issued with any further fines.

At the federal level, the **German Supervisory Authority** imposed a fine of 1,500 EUR in application of the GDPR. The fine was issued in December 2018 due to a failure to cooperate with the Authority.

Other fines issued under the GDPR in Germany in 2018 included:

- two fines issued by the federal state of **Mecklenburg-Western Pomerania**, totalling 1,500 EUR;
- thirty-six fines issued by the Data Protection Authority of **North Rhine-Westphalia**, under Article 83(5) of the GDPR, amounting to 15,600 EUR;
- six fines issued by the DPA of the federal state of **Saarland**. These included one fine issued under Article 58(1) of the GDPR, two issued under Article 58(2) and three issued under Article 83(5).

[1] This non-exhaustive list is based on information received from the national Supervisory Authorities.

6.2.1.3. Sweden

At the end of May 2018, the Swedish Data Protection Authority initiated an audit of several organisations to see whether data protection officers had been appointed in accordance with the GDPR. After examining more than 350 companies and authorities, the audit results were published in October 2018.

The audit showed that the majority of the authorities and companies investigated had notified and appointed a data protection officer on time. However, the Swedish DPA identified deficiencies in approximately 16% of cases. There was only a marginal difference in compliance between public authorities and private sector companies.

Out of 66 scrutinised cases, the Swedish DPA issued 57 reprimands. In two other cases, the DPA issued the audited organisation with an order to comply, while seven cases were closed without further measures taken.

6.3. DPA SURVEY – BUDGET AND STAFF

Under the new legal framework, SAs have received new harmonised tasks and powers. They wield greater enforcement and investigation powers, they handle individuals' complaints, have to promote awareness on data protection law and are also required to cooperate with the other Supervisory Authorities. This implies a need for increased budgets and more staff members.

6.3.1 Budget

Based on information provided by SAs from 26 EEA countries and the EDPS, an increase in the budget for 2018 and 2019 has in most cases occurred. However, the budget of two SAs decreased, while in three cases there were no changes. According to information provided by the respective SAs, the lack of changes can be explained by the application of biannual plans spanning this period.

Under the new legal framework, SAs have received new harmonised tasks and powers. This implies a need for increased budgets and more staff members.

Most of the SAs (17) stated that they required a budget increase of around 30-50% to perform their duties. However, almost none of the SAs received the requested amount. In some extreme cases, SAs have a need for up to double their current budget.

6.3.2 Staffing

Based on information provided by SAs from 26 EEA countries and the EDPS, a majority of SAs have increased their staff numbers. However, in eight SAs the number of employees did not increase, while in one SA there was a decrease in staff numbers. Differences in personnel requirements across SAs is to be expected, given the varied remits of the SAs.

7

Transparency and access to documents

Transparency is a core principle of the EDPB. As an EU institution, the EDPB is subject to Article 15 of the TFEU and Regulation 1049/2001 on public access to documents. Article 76(2) of the GDPR and Article 32 of the EDPB's Rules of Procedure reinforce this requirement.

Upholding the principle of transparency means that any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State has a right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities.

In exceptional cases, the EDPB can refuse to disclose a document, or part of it. The reasons for refusal and other procedural rules are outlined in the EU Public Access Regulation.

In 2018, the number of public access requests received for documents held by the EDPB was ten.

To ensure transparency, the EDPB also publishes the agendas and plenary sessions attended by the EDPB on its website. In 2019, the EDPB will continue to implement measures designed to increase the transparency of its work.

All citizens who believe they have been unjustifiably refused access can lodge a complaint with the European Ombudsman, or bring an action before the Court of Justice of the European Union.

8

Stakeholder consultation

8.1. PUBLIC CONSULTATIONS ON DRAFT GUIDANCE

The EDPB organises public consultations to gather the views and concerns of all interested stakeholders and citizens. In 2018, the EDPB issued three consultations on its draft Guidelines:

- In May, the EDPB opened a public consultation on the Guidelines on certification (1/2018);
- In November, the EDPB opened a public consultation on the Guidelines on the territorial scope of the GDPR (3/2018);
- In December, the EDPB opened a public consultation on the Annex 1 of the Guidelines on the accreditation of certification bodies (4/2018).

8.2. STAKEHOLDER SURVEY ON ADOPTED GUIDANCE

A survey was conducted on adopted guidance as part of the annual review of European Data Protection Board activities under Article 71 of the General Data Protection Regulation. It focused on 20 GDPR Guidelines with questions concerning both their content and the adoption process, with a view to establishing stakeholders' opinions on their quality and usefulness.

In order to increase the reach of the questionnaire and the diversity of those responding to it, the EDPB invited 114 pan-European organisations to participate in the survey. They represent different geographies, sectors and business sizes.

Fifty-three responses were submitted. The results showed that participants had consulted, on average, eight Guidelines. The majority of the contributors were based in Europe (41 entities) as opposed to ten headquartered in North America and two in the Asia-Pacific region.

The outcome of the survey confirms that Guidelines are seen as useful and pragmatic.

Sixty-five percent of stakeholders considered the Guidelines to be useful. While 45 percent considered them to be sufficiently pragmatic and operational for their needs, 23 percent called for improvement. For instance, they recommended shorter and more pragmatic guidance, not stricter than the GDPR, and to avoid contradictions between EDPB and national guidance. While half of the respondents judged the Guidelines to provide sufficient examples in their respective area of regulation, 16 percent called for the inclusion of more sophisticated case studies. Smaller businesses, with less expertise in data protection, favoured easier texts. The Guidelines were also judged positively as regards accessibility. Sixty-one percent of those who responded to the survey found the Guidelines easy to read, while 64 percent considered them easily accessible on the EDPB's website.

Most feedback concerning the consulting and drafting process of the Guidelines was positive or neutral. Some stakeholders encouraged the EDPB to increase opportunities to be involved and cooperate in the drafting of Guidelines.

The outcome of the survey confirms that, while the Guidelines are generally seen as useful, there is an understandable difference in their application depending on the sector, size and level of expertise of the stakeholder. The feedback was highly valued by the EDPB, as it moves to adopt further guidance in the next two years aimed at clarifying the GDPR provisions.

8.3. STAKEHOLDER EVENTS

The EDPB values the transparency of its activities. Its work programme, therefore, establishes the EDPB's commitment to creating increased opportunities for stakeholder engagement, such as the launch of stakeholder events.

During its last plenary meeting of 2018, the EDPB decided to organise two stakeholder events to collect views before adopting Guidelines on specific topics. The respective topics were the update of the 2010 Opinion of the Article 29 Working Party on the concepts of Controller and Processor and the elaboration of EDPB Guidelines on the Payment Services Directive (PSD2). The events were scheduled to take place in 2019.

9

Main objectives for 2019

Having turned one on 25 May 2019, the EDPB is now looking ahead, evaluating where its focus should be in 2019 and beyond.

9.1. LEGAL WORK PLAN

At the beginning of 2019, the EDPB adopted a two-year work programme for 2019-2020. This is based on the priority needs of all stakeholders, including the EU legislator, as identified by EDPB members. Three areas of interest were identified for the coming two years, as outlined below.

The EDPB adopted a two-year work programme for 2019-2020.

9.1.1. Further Guidance

The EDPB will adopt further Guidelines to ensure consistent interpretation of the GDPR across the EU, enabling stakeholders and Supervisory Authorities to apply the provisions of the GDPR in a harmonised manner.

In 2019 and 2020, the EDPB aims to focus on data subjects' rights, the concept of the controller and processor and legitimate interest. The EDPB will also consider technologies such as connected vehicles, blockchain, artificial intelligence and digital assistants, video surveillance, search engine delisting and data protection by design and by default.

9.1.2. Advisory Role to the European Commission

The EDPB will continue to advise the Commission on issues such as cross-border data access requests for e-Evidence, the revision or introduction of adequacy decisions for data transfers to third countries and any possible revision of the EU-Canada Passenger Name Record (PNR) agreement.

9.1.3. Consistency Measures

In cross-border cases where consensus cannot be found between the Lead SAs and Concerned SAs within the relevant cooperation procedure, the EDPB will act as a dispute resolution body and issue binding decisions.

In addition, the EDPB will continue to deliver Consistency Opinions to Supervisory Authorities in line with Article 64 of the GDPR. These include cases such as the SAs' draft approval of cross-border codes of conduct, certification criteria and binding corporate rules to ensure the transfer of data within multinationals.

9.2. COMMUNICATIONS

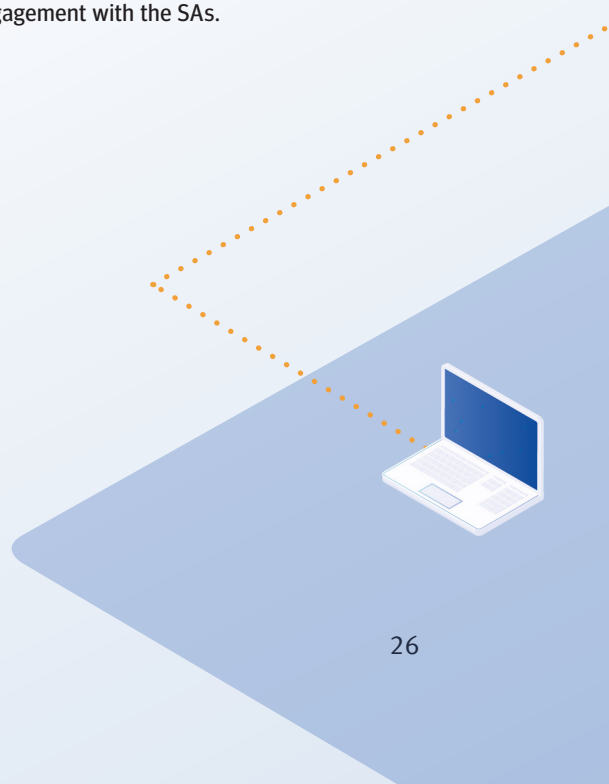
The EDPB ensures full transparency of its work among media, the public and stakeholders from across the public and private sectors. This is particularly vital at a time when there is a heightened public focus on data protection and privacy issues.

In 2019, the EDPB will continue this mission by deepening existing stakeholder relationships and developing new ones with relevant parties.

The EDPB Members are fully committed to continuing their participation in relevant conferences and speaking engagements, as well as maintaining a strong social media presence to drive public engagement with the EDPB's activities.

The EDPB will continue its mission by deepening existing stakeholder relationships and developing new ones with relevant parties.

Given that a significant part of the EDPB's work relies on its cooperation with the Supervisory Authorities, the EDPB is keen to support a harmonised communication approach. This will be further developed in 2019, via the network of Data Protection Authorities press and communications officers, as well as through supporting the EDPB Chair in her outreach and engagement with the SAs.



10

Contact details

Postal address:
Rue Wiertz 60, B-1047 Brussels

Office address:
Rue Montoyer 30, B-1000 Brussels

Email:
edpb@edpb.europa.eu

11

Annexes

11.1. GENERAL GUIDANCE ADOPTED IN 2018

1. Guidelines on consent under Regulation 2016/679, WP259 rev.01
2. Guidelines on transparency under Regulation 2016/679, WP260 rev.01
3. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
4. Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
5. Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01
6. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01
7. Guidelines on Data Protection Officers ('DPO'), WP243 rev.01
8. Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01
9. Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
10. Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01
11. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264
12. Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265
13. Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01
14. Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01
15. Working Document on Adequacy Referential, WP 254 rev.01
16. Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, WP 253
17. EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679
18. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
19. EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version for public consultation
20. EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

11.2. EXPERT SUBGROUPS: SCOPE OF MANDATE

NAME OF SUBGROUP	SCOPE OF MANDATE
Borders, Travel & Law Enforcement (BTLE) Expert Subgroup	• Law enforcement directive • Cross-border requests for e-evidence • Adequacy Decisions, access to transferred data by law enforcement and national intelligence authorities in third countries (e.g. Privacy Shield) • Passenger Name Records (PNR) • Border controls • Preparation of the coordinated supervision under Art. 62 1725/2018
Compliance, e-Government and Health Expert Subgroup	• Code of conduct, certification and accreditation • Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates • Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates • Compliance with public law and eGovernment • Health
Cooperation Expert Subgroup	• General focus on procedures of the GDPR • Guidance on procedural questions • International mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50)
Coordinators Expert Subgroup	• General coordination between the Expert Subgroup Coordinators • Coordination on the annual Expert Subgroup working plan

NAME OF SUBGROUP	SCOPE OF MANDATE
Enforcement Expert Subgroup	• Including exchange of information on concrete cases • Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII of the GDPR, including mapping/analysing possible updates of existing Cooperation subgroup tools) • Monitoring of investigation activities • Practical questions on investigations • Guidance on the application of Chapter VIII of the GDPR together with the Fining TF
Financial Matters Expert Subgroup	Application of data protection principles in the financial sector, more specifically: • Automatic exchange of personal data for tax purposes • FATCA • Administrative arrangements for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities for cooperation purposes (ESMA) Interplay between Second Payment Services Directive (PSD2) and GDPR
International Transfers Expert Subgroup	Guidance on Chapter V: International transfer tools and policy issues, more specifically: • Review European Commission Adequacy decisions • Guidelines on Art. 46 of the GDPR and review of administrative arrangements between public authorities and bodies (e.g. ESMA) • Codes of conduct and certification as transfer tools • Art. 48 of the GDPR together with BTLE ESG • Art. 50 of the GDPR together with Cooperation ESG • Guidelines on territorial scope and the interplay with Chapter V of the GDPR - interaction with Key Provisions ESG • Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 of the GDPR

NAME OF SUBGROUP	SCOPE OF MANDATE
IT Users Expert Subgroup	Developing and testing IT tools used by the EDPB with a practical focus: collecting feedback on the IT system from users, adapting the systems and manuals as well as discussing other business needs including tele- and videoconference systems
Key Provisions Expert Subgroup	Guidance on Chapters I (e.g. scope, definitions like LSA and large scale processing) and II (main principles) and on core concepts and principles of the GDPR, including Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with Compliance Tools ESG, Enforcement ESG and Technology ESG) and IX
Social Media Expert Subgroup	• Analyzing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing • Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals • Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons. • Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance

NAME OF SUBGROUP	SCOPE OF MANDATE
Strategic Advisory Expert Subgroup	• Guidance on strategic questions affecting the whole EDPB (including the discussion on the work plans of the ESGs) • Clarification of questions that could not be resolved in the ESG
Taskforce on Administrative Fines	Development of guidelines on the harmonisation of the calculation of fines
Technology Expert Subgroup	• Technology, innovation, information security, confidentiality of communication in general • ePrivacy, encryption • DPIA and data breach notifications • Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments • Providing input on technology matters relevant to other ESGs

@eu_edpb
eu-edpb
edpb.europa.eu

edpb
European Data Protection Board